국제학석사학위논문

Digital Commerce in international trade relations; focusing on data localization

국제무역관계에서의 디지털 커머스;
데이터로컬리제이션을 중심으로

2017년 8월

서울대학교 국제대학원

국제학과 국제통상 전공

고 태 경

Digital commerce in international trade relations; focusing on data localization

A thesis Presented

By

Taekyung Koh

to

A dissertation submitted in partial fulfillment
of the requirements for the degree of Master
of International Studies in the subject
of International Commerce

Graduate School of International Studies

Seoul National University

Seoul, Republic of Korea

August 2017

Digital commerce in international trade relations; focusing on data localization

국제무역 관계에서의 디지털 커머스: 데이터로컬리제이션을 중심으로

지도교수 안덕근

이 논문을 국제학석사학위논문으로 제출함

2017년 08월

서울대학교 국제대학원
국제학과 국제통상전공
고태경

고태경의 국제학석사학위논문을 인준함

2017년 08월

위 원 장 이영섭 (印)

부위원장 박태호 (印)

위 원 안덕근 (印)

THESIS ACCEPTANCE CERTIFICATE

The undersigned, appointed by

The Graduate School of International Studies
Seoul National University

Have examined a thesis entitled

Digital commerce in international trade relations; focusing on data localization

Presented by **Taekyung Koh**

Candidate for the degree of Master of International Studies and hereby certify that it is worthy of acceptance

Signature Committee Chair	**Rhee, Yeongseop**
Signature Committee Vice Chair	**Bark, Tae-Ho**
Signature Committee Member	**Ahn, Dukgeun**

Date: August 2017

Abstract

Today, data transfers are considered as one of the most important yet controversial topics in many countries. Although no one disagrees on the importance of cross-border data transfers, many countries adopt or maintain data localization measures for different purposes such as to protect citizens' privacy and security, to develop their economies, or simply to enforce domestic laws. Korea is one of those countries that maintain strict data localization measures on personal information, location information and spatial data. Although it is true that these types of measures are necessary in order to protect privacy and personal information, they may act as hurdles to development of digital economy, including location based services and cloud computing industries. Thus, it is important for countries to strive to remove these hurdles and cooperate to lay out multilateral rules on data transfers. In fact, recent FTAs such as KORUS FTA and Trans Pacific Partnership (TPP) include provisions on cross-border data transfers, and especially TPP e-commerce chapter specifically addresses server localization issue. In this aspect, this paper analyzes data localization measures based on different purposes, conducts in-depth study on Korean data localization measures, and then examines relevant FTA chapters to propose new norms for those countries adhering to strict data localization laws.

Table of Contents

Introduction

World has become digitalized and digital trade is gaining popularity. According to USTR, the number of internet using population worldwide has been increased from 1.5 billion to 3 billion over past six years, and in response to this leap in internet using population, trade is gradually shifting from more conventional method to digitalized one. Since its establishment, WTO members have agreed to eliminate tariffs on information and technology related goods through Information Technology Act (ITA) in 1996, and through Basic Telecommunications Agreement and reference paper, members tried to remove unnecessary discriminatory actions of public telecommunications networks and services between member states. Indeed, after ITA I agreement, trade in IT related goods increased 11.5 percent between 1997 and 2005.[1] However, it was not until since 1998, at the second ministerial conference at Geneva, WTO began to seriously address digital commerce issues. It set up WTO work programme on e-commerce, but this has played very few roles in terms of liberalizing digital commerce, other than simply agreeing on 'no tariffs on electronic transmissions.' Even this duty free moratorium is provisional and the concept of 'electronic transmission' is vague.[2]

---

[1] Geunhwa Lee, *ITA II in effect and its implication* (KITA, 2016), 8
[2] Hanyoung Lee, *Trade Rules on Electronic Trade in Services: The Outputs of WTO and FTAs*

Under WTO, one of the most perplexing questions have been whether to apply GATT or GATS rules for digital commerce, and WTO dispute case, DS285 case on online gambling clarified that under certain circumstances, GATS may apply to e-commerce issues, thus electronically transmitted goods and services should be treated more or less equal. This case further elaborated that GATS mode 1, cross-border supply of services apply to electronic service such as internet gambling.[3] Furthermore, DS363 case on China-Audiovisuals touched upon technology neutrality issue, thus clarifying that no differential treatment shall be given to electronically versus physically delivered goods and services.

However, even though these two dispute settlement cases touched upon new dimension of e-commerce rules, these cases did not effectively address wide variety of issues concerning digital commerce. In fact, it was FTAs that rigorously expanded liberalization criteria of e-commerce and tried to come up with more progressive and realistic rules governing e-commerce. Most of recent US led FTAs, include separate chapter on e-commerce, and KORUS FTA and TPP includes very progressive commitments on e-commerce. Especially, TPP is the first FTA to touch upon data localization issue, which has been prevailed over decades.

(通商法律, 2008), 121-122

[3] Sacha Wunsch-Vincent, *The Internet, cross-border trade in services, and the GATS: lessons from US–Gambling* (World Trade Review, 2006), 319-355

Data localization refers to domestic laws or regulations that force localization of data, limiting the storage, movement and processing of data to specific jurisdictions, or limiting companies that can operate with countries' data.[4] Basically, this practice is prohibiting transfer of data out of border or giving permissions only to a few companies to have access to data. Data localization practices are executed in diverse ways, by restricting server location by compelling foreign services providers to build and operate data servers within the border, by controlling enterprises or individuals to export data, or by targeting specific sectors' data such as health and finance.

Indeed, both socially and economically, data localization's negative impact has been tested. According to Mishra's study, data localization practices significantly harm economies by reducing competitiveness and productivity of businesses and consumers in the world trade system where roughly a half of all services trade are made through the ICT industry.[5] The research also notes that data localization laws do not enhance data security but contrastingly make it more vulnerable to local surveillance and security risks. Thus, the paper recommends that countries should take globalization approach in digital space, which is prioritizing international cooperation on free data flow while giving

[4] Jonah Force Hill. *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders* (Cyber Governance, 2014), 3

[5] Neha Mishra. *Data localization laws in a digital world* (The Public Sphere, 2016), 141-142

specific attention to local interests.

European Centre for International Political Economy (ECIPE) conducted quantitative analysis on the impact of data localization restrictions on nations' economy, and according to their analysis, current data localization measures in many countries are likely to lower those countries' GDP substantially, and also would likely to trigger welfare losses.

Research Objectives & Methods

There is yet no multilateral rule that covers wide variety of issues concerning digital trade, but rather, bilateral and Mega FTAs are filling this gap recently. KORUS FTA and TPP include very advanced provisions governing e-commerce, and especially TPP includes rules on cross-border data transfer, prohibition of source code requirements and location of computing servers etc. In fact, among these progressions made under TPP, banning forced server localization is one of the most noteworthy achievements, because localization requirement is a protective measure that hampers free flow of information cross-border, double edge sword harming both consumers and service providers. Furthermore, today is the era of cloud computing and ICT, and localization requirement greatly undermines many benefits that these technological developments provide.

In this regard, this paper examines three points: 1) Recent emergence of data localization laws in many countries, especially focusing on Korean case, and their economic implications 2) Contrasting perspectives of EU and US on data localization, 3) How TPP addresses anti-localization requirement and security. By examining these points, this paper tries to answer following questions:

1) What is the implication behind countries' adopting data localization laws? 2) To what extent and how data localization laws in each country, especially focusing on Korean case, are likely to affect global digital trade and economy? 3) Are TPP rules enough to shift countries from adopting localization requirements and encourage cross-border data transfers globally?

To fulfill research objectives mentioned above, first, this paper will thoroughly analyze different perspectives of major powers, US and EU, on data localization, privacy, and transfer of information cross-border. Then, the paper will examine recent emergence of data localization laws in different categories, especially focusing on South Korean case. Then, lastly, this paper will study relevant FTA provisions, including TPP, and study how these new rules can counter balance protective laws in each country, and if there is any, what are the limitations of these FTAs in terms of liberalizing cross-border data flow.

EU and US perspectives on data localization

Since 1980s, the United States have been a leading proponent of free flow of information. Two major powers, European Union (EU) and the United States (US) took different approaches with regards to data localization. For instance, at TISA negotiation, a multilateral services trade agreement which EU and the US participate, both EU and the US agreed to include language that permits free flow of information. However, as negotiation proceeds, US urged more stringent rule on free transfer of information in electronic forms, whereas EU wanted to save some room for the protection of privacy and personal data. In TTIP negotiation as well, even though EU agreed to negotiate provisions on the free data transfer, they have changed their position to not include language that may go against EU's stance on privacy and data protection.

Also, their trade agreements with other countries show their different approaches to free flow of information. First FTA to include language 'free flow of information in the electronic commerce' was KORUS FTA, led by the United States. Article 15.8 reads as follows; '*The Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.'*[6] Another important multilateral FTA, TPP, which was originally led by the United States, further strengthened this language of

[6] KORUS FTA Article 15.8: Cross-Border Information Flows

KORUS FTA by adopting data localization prohibitions and by using more obligatory connotation. TPP will be discussed in detail in the later part of this paper. On the other hand, EU led FTAs such as EU-Chile, EU-Korea FTA do not include language on free flow of information in their electronic commerce chapters.

The principal reason that these two parties were unable to reach conclusion on trade agreements to set transfer of information free was because there has been no consensus made for whether all information flows are traded services.[7] Also, GATS rules allow individual country to adopt trade restrictions if those restrictions are necessary to protect privacy, intellectual property, public health and public morals, and there is a promise that these restrictions are non-discriminatory between WTO member countries.[8]

Another important reason is that two parties, EU and the US, do not share the same definition in law, on 'online privacy.' US law considers online privacy as a consumer right and focuses on freedom of access to data, whereas the EU law sees this as a human and consumer right that government should protect. EU's Data Protection Directive bans transfer of data cross-border, except for the

---

[7] Susan Aaranson. *Why Trade Agreements are not Setting Information Free*: *The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security* (World Trade Review, 2015), 3

[8] Jack Goldsmith and Tim Wu. *Who Controls the Internet? Illusions of a Borderless World* (New York: Oxford University Press, 2006) ,142-181

cases when EU judges that there is enough protection for privacy.[9]

Even at this discrepancy in their laws, two parties have signed on 'Safe Harbor Agreement' in year 2000, which authorizes free flow of information to those certified organizations which meet standards of each party's privacy protection schemes. Thus, it is quite clear that both of them, at least superficially, clearly shared an idea of liberalizing cross-border data transfer.

In June 2013, a former member of CIA, Edward Snowden, revealed that US intelligence service is engaged in extensive surveillance over phone calls and internet data of other countries' citizens, including those of EU. This divulgation outraged many countries, and domestic interests to localize data within the borders to protect their citizens' private data over US surveillance prevailed. This was in this context that EU challenged validity of Safe Harbor Agreement because with Snowden's allegation, it has been found that many of the American companies that were certified to meet EU standards of privacy protection under the Safe Harbor Agreement were in fact handing out European citizens' personal data to US intelligence service.[10] Thus, the gap in perspectives on free flow of data between EU and US got widened even more

---

[9] Susan Aaranson. *Why Trade Agreements are not Setting Information Free*: *The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security* (World Trade Review, 2015), 12

[10] Susan Aaranson. *Why Trade Agreements are not Setting Information Free*: *The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights and National Security* (World Trade Review, 2015), 21

after this incident. In October 2013, the European Parliament's Civil Liberties, Justice and Home Affairs Committee decided to reform EU data protection law and adopted General Data Protection Regulation (GDPR), which prohibits data transfer to overseas countries where the local authorities can have access to the data from EU.[11]

Especially in Germany, shortly after the US NSA revelations, voices to limit data flow circuits only within the territory have been aroused. The German Data Protection Commissioners expressed disapproving international data transfers until foreign national intelligence services abide by German data protection and German government authorizes this. [12] Also, Deutsche Telekom, a telecommunications company partially owned by German government, launched a service called 'e-mail made in Germany,' and in October 2013, they proposed intra-national data transfers should be made only through German networks. Moreover, in following February, German chancellor Angela Merkel proposed setting up of Europe's own internet infrastructure to limit data transfers out of Europe.

Along with Germany, French government expressed vehement outrage over US intelligence service's spying. In fact, even before Snowden allegation, France

[11] Anupam Chander and Uyên P. Lê. *Data Nationalism* (Emory Law Journal), 690

[12] Anupam Chander and Uyên P. Lê. *Data Nationalism* (Emory Law Journal), 692

was working on ‘data tax’ to data services suppliers, and building its own national cloud called ‘sovereign cloud,’ and government has provided subsidies to two French cloud computing companies to develop this national cloud. US surveillance has spurred this French government’s ambition to localize data internally, and the government declared its plan to build a France of digital sovereignty.[13]

Different categories of data localization – based on purposes

Countries have many purposes behind adopting data localization rules. Like European countries, countries use data localization to protect user’s privacy and security, to counteract against foreign surveillance, and to protect national security. Sometimes, data localization measures are used for economic development or domestic law enforcement purposes. Also in some cases, different purposes overlap. In this section, this paper analyzes data localization measures of different countries based on different rationales.

A. National security and counteraction against foreign surveillance

Along with European countries, India’s data localization measures put heavy emphasis on national security and protection against foreign surveillance. For instance, Public Records Act bans transference of public records out of India,

[13] Anupam Chander and Uyên P. Lê. *Data Nationalism* (Emory Law Journal), 691

except for few public purposes, and government e-mails are prohibited to be transferred abroad. Also, Indian National Council has proposed that e-mail host servers to be located in India, and to prohibit servers located outside of India to scan Indian data. Russian Federal Laws No. 97 requires information organizers, or often times called 'bloggers,' to store all kinds of information regarding their jobs such as transmission, delivery and processing of texts, images, sounds, etc., for at least six months in Russia. Also, the Russian Ministry of Communications has written an order that requires telecommunications and internet service providers to save data locally or at least a copy of it for minimum 12 hours. Ironically, this has served Russian intelligence services to have direct access to data on domestic and foreign websites such as G-mail and Yandex.

B. User's privacy and security

Malaysia's Personal Data Protection Act limits transfer of personal data outside the country only to specific conditions, conditions specified by the minister, or agreed by the data subject. Another case is that Russia's Federal Law No.242 bans services providers to store Russian personal data out of Russian territory, and the service providers must reveal locations of datacenters. Proposed law in France to tax data services providers (depending on their compliance level to the French privacy and personal information protection regime) is another peculiar form of data localization for privacy protection purpose.

C. Economic development

Underdeveloped countries sometimes adopt data localization measures to nurture their IT sectors. By giving incentives to domestic service providers through data localization measures, these countries try to earn some time for domestic IT firms to gain competitiveness. Nigeria's case is a good example for this. Nigerian National Information Technology Development Agency has developed a guideline obliging ICT companies to host and save all Nigerian consumer information and data locally. Also, Nigerian government has set a local content and hardware usage target for IT industry, meaning that IT services providers have to adopt about 50% of locally provided goods and services to operate in Nigeria.

D. Domestic law enforcement purpose

Sometimes, government's purpose for data localization regulations is neither for privacy and personal information protection nor for national security or development purposes. Simply to enforce certain law, countries use data localization practices. Data localization provision in Vietnamese Decree 72 is an example of this. This law is basically to suspend the use of internet services to criticize the government and against national security and social order. This law requires internet service providers to store a copy of all the information they retain in Vietnamese territory, in order for Vietnamese government to

easily inspect these internet websites and networks.

Korea and data localization

A. data localization measures

Korea too, is a country with strong regulations on internet and data transfers. Similar to many other countries, Korea's purpose of data localization measures is to protect user's privacy and national security. However, what is distinctive about Korea's case is that Korea besides strong personal information protection, the country regulates heavily on spatial and location information for national security reasons. In fact, Korea has not strengthened its data protection laws or regulations in reaction to US NSA surveillance, some of the data control laws were in action since 1960s, after the seize of fire in Korean peninsula.

Three of the major laws covering data regulation and localization requirements in Korea are Personal Information Protection Act, so called PIPA of 2011, Act on the Protection of Location Information, and Korean Land Survey Act drafted in 1961, post-war era.

i. Personal Information Protection Act (PIPA)

PIPA is drafted to protect personal information of Korean citizens, and it applies to entities that handle or process personal information for business purposes

including persons, organizations and corporations.[14]

PIPA regulates the collection, use, provision, outsourcing, storage and obstruction of personal information including users' names, addresses, photographs etc.[15] One noteworthy point is that although PIPA does not specifically outlines whether the law applies to foreign entities, it clearly concerns about whether the foreign companies are targeting Korean users. Thus, the law applies to the foreign enterprises handling Korean citizens' user data.

PIPA includes regulation for data exports, and this is covered in the article 17(3) of the Act;

'When a personal information manager provides a third person at any overseas location with personal information, he/she shall notify a subject of information of the matters referred to in each sub paragraph of paragraph (2) and obtain the consent thereto, and shall not enter into a contract concerning the trans-border transfer of personal information stipulating any details contravening this Act.'[16]

---

[14] Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S. Keh and In Hwan Lee. "Data protection in South Korea: overview" https://content.next.westlaw.com/2-579 7926?transitionType=Default&contextData=(sc.Default)&__lrTS=20170506074209285&firstPage=true&bhcp=1, (July 15 2015)

[15] Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S. Keh and In Hwan Lee, "Data protection in South Korea: overview" (July 15 2015)

[16] Personal Information Protection Act Article 17(3) http://elaw.klri.re.kr/kor_service/lawView.do?hseq=35739&lang=ENG

Thus, in case of exportation of personal information, notification requirement to the information subject should be carried out beforehand.

Entities handling personal information, herein the Act referred as a personal information manager, should obtain the consent of an information owner before transferring the data, and also the following information relevant to the transfer:

1 A recipient of personal information

2 Purposes for which a recipient of personal information uses such information

3 Items of personal information to provide

4 Period for which a recipient of personal information holds and uses such information

5 The fact that an owner of information has a right to reject to give his/her consent and details of a disadvantage, if any, due to his/ her rejection to give consent.[17]

ii. Act on the Protection, Use of Location Information

Along with PIPA, Korea stringently regulates collection of location information of persons or things. Article 15 of the act stipulates that collection, use, or providing of an individual or mobile object without the consent of that

---

[17] Personal Information Protection Act Article 17(2)
http://elaw.klri.re.kr/kor_service/lawView.do?hseq=35739&lang=ENG

individual or the owner of the object is prohibited.[18] Thus, under this law, anonymous person's location information, too, should be protected and the same applies for non-living object's location. No other country has this kind of strict law regulating location information, and most other countries do not have separate law on protection of location information. South Korea's this strict regulation on location information can be hurdle to the development of LBS (location based service) industry in Korea.[19]

iii. Korean Spatial Data Protection Act

Korea has a strict spatial data protection act and the act's official title is *Act on the establishment, management, etc. of spatial data*. This law has its origin in post Korean war era, in 1961, South Korean government enacted the Land Act to prevent enemies or hostile entities from obtaining map of the country.[20] This act has been amended in 2009 and renamed as the Act on Land Survey, and amended several more times thereafter.

Article 16 of the act regulates fundamental land survey results abroad;

> *16(1). No person shall take abroad maps, etc. or photos produced for the purpose of survey, among the results of a fundamental survey without*

---

18 Act on the Protection, Use, Etc. of Location Information. Article 15 http://elaw.klri.re.kr/kor_service/lawView.do?hseq=33741&lang=ENG

19 Yoonryung, Eom,. *A Study on the Geolocation Data Protection Act – Focusing on Anonymous Geolocation Data* (Yonsei Medicine, Science Technology and Law, 2014), 54

20 Anupam Chander and Uyên P. Lê. *Data Nationalism* (Emory Law Journal), 703

permission of the Minister of Land, Infrastructure and Transport. That same cases shall not apply to cases prescribed by Presidential Decree, such as where the results of fundamental survey are exchanged with foreign governments.

16(2). No person shall take abroad the results of a fundamental survey in cases of falling under any subparagraph of Article 14(3), where it is likely to harm national security or other important national interests, and where it is prescribed as a confidential matter, such as one being kept secret, inspection of which is restricted and so on under other Acts and subordinate statues. That the same shall not apply where the decision to take them abroad is made by a consultative body organized by the Minister of Land, Infrastructure and Transport with the heads of the relevant agencies, including the Minister of Science, ICT, and Future Planning, the Minister of Foreign Affairs, the Minister of Unification, the Minister of National Defense, the Minister of Security and Public Administration, the Minister of Trade, Industry and Energy, the Director of the National Intelligence Service, etc.

16(3). Matters necessary for the organization, operation, etc. of the consultative body mentioned in the provision to paragraph (2) shall be

prescribed by Presidential Decree.[21]

Thus, as can be seen from above, land surveillance data are strictly forbidden to be exported. This is in part understandable considering special situation in Korean peninsula, where the country is divided in half and seize of fire has not been really made yet. Nonetheless, this strict regulation on data exportation make it difficult for foreign ICT companies, such as Google, to operate maps services in Korean territory. In fact, recently in 2016, Google and the South Korean government have failed to meet compromise over the company's exportation of maps data to the server located out of country. Korean government has reaffirmed that it cannot allow Google to operate mapping services in Korea and also to export mapping data of Korea to the US unless Google erases information on certain military or national security basins of Korea. American government, has expressed its opinions on the issue through commerce summit meetings with Korean government since 2008, and is arguing that this regulation in Korean law is discrimination against foreign IT companies.[22]

GATT and GATS takes different approach with regards to National Treatment. Whereas GATT takes obligatory words regarding national treatment, GATS

21 Act on the Establishment, Management, etc. of Spatial Data Article 16. http://elaw.klri.re.kr/eng_service/lawView.do?hseq=32771&lang=ENG

22 "chance is low that Google would like to reapply for mapping data exportation to Korean government" http://www.huffingtonpost.kr/2016/06/04/story_n_10293658.html (June 4 2016)

national treatment is not obligatory, but it depends on countries' specific commitments on schedules. Korea's GATS schedule specifies map-making services' mode 1 supply, cross-border supply, is 'unbound' by the limitations on national treatment, meaning that the country is free to introduce or maintain measures regarding map-making services inconsistent with national treatment. Therefore, in Korea's case with Google, the issue is not on national treatment, but on MFN obligation.

B. Economic impact of Korean data localization measures

ECIPE study on data localization predicted that current data localization measure would likely to lower Korean GDP by 0.4%, and if Korea expands data localization requirements to all sectors of economy, then Korean GDP would be lowered by 1.1%. Also, current Korean legislation can lower investments by 0.5% and may lead to the welfare loss of workers, approximately 20% welfare loss per worker.[23]

In a following study, they have specified TFP changes triggered by data processing regulations by sectors, and have determined that business services, services, and communications sectors are most vulnerable to TFP losses in

[23] Erik Van der Marel, Hosuk Lee-Makiyama and Matthias Bauer. *The Costs of Data Localisation: A Friendly Fire on Economic Recovery* (ECIPE Occasional Paper, 2014), 2

Korea due to data localization requirements.[24]

Table 1. Korean TFP change as a consequence of data processing regulations

Sector	TFP changes
All sectors	-0.35
Communication	-2.13
Business services	-0.84
Services	-0.51
Other business and ICT sectors	-0.46
Financial and insurance services	-0.34
Machinery	-0.33
Other consumer services	-0.32
Public services, dwellings	-0.27
Distribution	-0.25
water	-0.23
transport	-0.22
construction	-0.16
Manufacturers	-0.16
Metal products	-0.13
Goods	-0.12

Thus, in sum, it is more likely that development of services driven industries such as communications, business services and ICT sector are more severely interrupted by data localization and processing regulations in Korea.

[24] Erik van der Marel, Matthias Bauer, Hosuk Lee-Makiyama and Bert Verschelde. A *methodology to estimate the costs of data regulations.* (International Economics, 2016), 29

Within the ICT sector, cloud computing is one of the areas that is directly hit by the data localization requirement, because cloud computing is an internet based technology, which the information stored in servers are provided to clients living in diverse parts of the world through the internet. In Etro's study on cloud computing and its economic influence, he has clarified three important benefits of cloud computing including business creation and macroeconomic performance, job creation especially in SMEs, job reallocation in the ICT sector, and the cost saving influences on public finances such as in hospitals, healthcare, education and government agencies.[25] Thus, by restricting data transfers, economies may face difficulties in vast different sectors, not only services and ICT, but also in manufacturing, retail, finance, and even public sectors may be vulnerable to hardships.

Another newly emerging industry that can be influenced by data localization measures can be drone industry. Drone market is expected to develop approximately to 17.5 billion USD in 2020. However, localization measures such as Korean regulations on protection of location information can act as hurdles to development of drone industry in the market. For instance, difficulty collecting location information data of persons or mobile objects make it difficult for IoT service providers to develop LBS technology based on location

[25] Federico Etro, "The Economics of Cloud Computing," in *Cloud Computing Service and Deployment Models Layers and Management* (Pennsylvania: Business Science Reference, 2013)

information.[26]

New global norm for data localization

A. Development of e-commerce rules in bilateral FTAs

Although data localization issue has not been dealt until TPP negotiation, earlier FTAs have paved road for the development of e-commerce rules. Since the US FTA with Jordan in 2000, US led FTAs started to incorporate e-commerce provisions. The first FTA to address elimination of customs duties regarding electronically transferred digital products was US-Singapore FTA, and in this same FTA, MFN obligation to digital products has been introduced as well.[27] Later, several FTAs such as US-Peru FTA and US-Colombia FTA began to incorporate consumer protection sections, affirming that the parties should recognize the importance of consumer protection measures in e-commerce and cooperation between each other's national consumer protection agencies.[28]

However, it was not until KORUS FTA, that FTAs began to talk seriously about open access and free flow of information, which are essential parts of data transfers. Article 15.7 on open access and use of the internet recommends

---

[26] Baek Soo-Won, Drone, Unmanned Aircraft, Privacy by Design, Done Rgulation, Personal Information Protection (SungKyunKwan Law Review, 2016), 318

[27] Brian Bieron, Usman Ahmed, *Regulating E-commerce through Internatioanl Policy: Understanding the International Trade Law Issues of E-commerce,* Journal of World Trade

[28] US-Peru FTA, Article 15.5: Consumer Protection ; US-Colombia TA, Article 15.5: Consumer Protection

parties to recognize the importance of open access and use of the digital products, applications of consumers' choices, and encourages the competition among network providers.[29] In addition to this, Article 15.8 on cross-border information flows is noteworthy;

> *Recognizing the importance of the free flow of information in facilitating trade… the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.*

As can be seen from the language 'shall endeavor,' KORUS FTA does not obligate cross-border flow of information to be set free from the barriers. Although it is not binding in language, it is still meaningful that for the first time, FTA parties began to recognize the importance of free cross-border information flow.

B. Data localization rule in TPP

So far, there has been no multilateral or bilateral trade negotiation addressing data and server localization issue. TPP is the first trade negotiation to address data localization issue, and heavily emphasizes services trade matters. Before examining TPP provisions on electronic commerce, this paper analyzes crucial points of TPP services trade chapter, which sets the baseline for the later part on

[29] KORUS FTA Article 15.7: Principles on Access to and Use of the Internet for Electronic Commerce

electronic commerce.

Under TPP, cross-border trade in services or cross-border supply of services is categorized into three different modes;

(a) from the territory of a Party into the territory of another Party;

(b) in the territory of a Party to a person of another Party;

(c) *by a national of a Party in the territory of another Party*[30]

In short, these three modes of cross-border supply of services mark international services trade between territories, persons and territory to persons. One thing noteworthy about this definition is the second point, which legitimizes services providers located out of counterpart's territory to provide services to citizens of that countering party.

Services trade chapter of TPP applies to domestic measures concerning not only the production, distribution, sale or the purchase of a service, but it also applies to the telecommunications network services and financial security matters.

The most important part of TPP services chapter and also one of the most relevant parts to the data localization issue are article 10.3 on National Treatment, article 10.4 on Most Favored Nation (MFN), and article 10.5 and 10.6 on market access and local presence, respectively. With regards to articles 10.3 and 10.4, just like goods trade, parties should treat foreign services and

[30] Trans-Pacific Partnership Article 10.1: Definitions

services suppliers equal to domestic suppliers, and in similar circumstances, no less favorable treatment shall be given to counter party's suppliers over other domestic and foreign suppliers.

TPP market access provision forbids domestic measures or practices that hinders fair market access by limiting the number of service suppliers, the total value of service transactions or assets by setting numerical quotas, or by restricting the total number of service operations or the number of employees in a specific service sector, or by requiring service suppliers to work with specific legal entity or joint venture to provide services.[31] In addition to these, TPP article 10.6 on local presence addresses that no party should force another party's service supplier to establish or maintain a representative office in their territory or to reside within the border to provide their services. Through these detailed articles on cross-border services trade, TPP aims to facilitate more open, and competitive ground for services trade.

TPP has a separate chapter on electronic commerce, more improved than KORUS FTA e-commerce chapter, and it is by far the most advanced chapter on e-commerce. Chapter 14 on electronic commerce specifically drafts variety of issues concerning digital commerce from non-discriminatory treatment of digital products to cross-border transfer of information by electronic means and

[31] Trans-Pacific Partnership Article 10.5: Market Access

location of computing facilities, etc.

TPP article 14.11 on cross-border transfer of information by electronic means aims to liberalize cross-border transfer of data by electronic means, including personal information, when the purpose of transfer is for business of a service supplier. However, it is important to note that 14.11.3 allows domestic laws and regulations to interrupt if necessary, to achieve public policy objective, and 14.11.1 urges parties to respect countering parties' domestic regulatory requirements. The article stipulates that even those measures for meeting public policy objectives should not pose discrimination or unnecessary restriction on trade, and the level of restrictions imposed should not surpass the level that is necessary for achieving the policy objective. One limitation of this article is that it is not clear from the article, the boundary of business of a covered person.

TPP article 14.13 on location of computing facilities is the provision that is directly related to data localization. This is indeed, one of the most interesting progresses made in TPP agreement, and no other previous FTAs have included this language. Article 14.13.2 reads as follow;

> *No party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business*

in that territory.[32]

Thus, in so far as business purposes, parties cannot force other contracting parties' service providers to set up a separate server or computing facilities in the territory to operate business in the country. However, similar to the article on cross-border transfer of information, parties may still adopt or maintain their own domestic laws or regulations for the use of computing facilities, such as regulations needed for the security and confidentiality of communications. Moreover, for the public policy objectives, parties can implement or maintain data or server localization regulations unless these regulations are applied in an arbitrary or discriminatory matter, pose unnecessary restriction on trade, or in a greater degree than what is needed for accomplishing the objective.

Along with the article 14.11 and 14.13, article 14.10 on principles on access to and use of the internet for electronic commerce, addresses the importance of freedom of online information or data consumption. This article is equivalent to article 15.7 of KORUS FTA, and indeed, not so much different from that of KORUS FTA in essence. It encourages governments to recognize the benefits of consumers having access to services provided in internet, using devices of their choices unless devices harm the network and allow consumer access to

[32] Trans-Pacific Partnership Article 14.13: Location of Computing Facilities

information on network management practices of internet service supplier.[33] Basically, the contents of this chapter is related to net-neutrality, which is about government and the internet services provider not discriminating against data on the internet based on websites, users, contents etc. Compared to other articles in the chapter, this article is rather soft and not binding, and unlike Trade in Services Agreement (TISA), which requires parties to adopt net-neutrality protection, this article on TPP text only asks for government understanding of net-neutrality and its benefits to consumers.[34]

Besides provisions on trade liberalization, TPP electronic commerce chapter also includes articles on online consumer protection and personal information protection. Article 14.7 on online consumer protection emphasizes the adoption or maintenance of consumer protection laws for online commercial activities, and the cooperation between national agencies to enhance consumer welfare. Through these laws on online consumer protection, the article notes that the parties should '*protect consumers from fraudulent and deceptive commercial activities…*'

The following article, article 14.8 is regarding personal information protection. Personal information protection is newly adopted in TPP electronic commerce

---

[33] Trans-Pacific Partnership Article 14.10: Principles on Access to and Use of Internet for Electronic Commerce

[34] Buruc Kilic & Tamir Israel, "The Highlights of the Trans-Pacific Partnership E-commerce Chapter," *Canadian Internet Policy and Public Interest Clinic,* (2015):8

chapter, and even KORUS FTA chapter on electronic commerce, the most advanced electronic commerce provision next to TPP, does not include separate article on personal information protection. Based on this article, parties should adopt or maintain domestic measures to protect personal information of the users of electronic commerce, but they should follow principles and guidelines of relevant international bodies when developing these laws.[35] Also, parties should adopt non-discriminatory practices in protecting personal information and should publish information on the personal information protections such as how users of electronic commerce can pursue remedies in case of breaches of personal information and how business can comply with any legal requirements.[36] Another point noteworthy about this article is that in 14.8.5, it includes language on development of mechanisms to promote compatibility between different legal approaches of different countries, to come up with a compromised legal system on personal information protection of electronic commerce users;

> *Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the*

---

[35] Trans-Pacific Partnership Article 14.8.2: Personal Information Protection
These domestic laws or measures may be comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy.

[36] Trans-Pacific Partnership Article 14.8.4: Personal Information Protection

development of mechanisms to promote compatibility between these different regimes… To this end, the Parties shall endeavour to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.

Therefore, while allowing legal instruments for personal information protection, TPP efforts to lay out middle ground with respect to personal information protection law that participating countries can compromise in the future.

Conclusion

Countries adopt data localization measures for diverse purposes, to protect their national security, personal information, develop their economy or simply to enforce their domestic laws. Like many other countries, Korea has data localization measures including PIPA, act on use of location information and act on spatial data. Due to special security situation in Korean peninsula, Korea puts heavy emphasis on spatial and location information data. However, such heavy regulations on data transfers negatively influence Korean economy, lowering GDP and triggering welfare losses. Especially strict regulations on location information and mapping data exports make certain Korean industries such as cloud computing, LBS industry, difficult to advance technology, and

make it extremely hard for foreign companies to operate services in Korea.

Meanwhile, recent FTAs, paved way for countries to move forward towards open and freer transfer of data, and especially TPP, which is so far the most advanced provision governing digital commerce, may suggest guideline to countries adopting or maintaining strong data localization measures. TPP article on digital commerce include provisions on server localization and free flow of information cross-border, and even though these rules do not completely prohibit countries from maintaining or adopting their domestic laws on data localization, these provisions are still meaningful because at least, they set the middle ground with respect to data localization.

In conclusion, Korea should endeavor to expand trade negotiations including rules similar to TPP and the government should try to loosen its regulations on data exports in order to facilitate cross-border information trade. Indeed, this is one of the most effective ways that the country can survive in the era of fourth industrial revolution.

Reference

English Literature

Aaronson, S. A. (2015). Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. World Trade Review, 14(04), 671-700.

Aaronson, S. A. (2016). The Digital Trade Imbalance and Its Implications for Internet Governance. Global Commission on Internet Governance Paper Series, (25).

Ahmed, Usman, and Anupam Chander. (2015). "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-Border Data Flows." *E15Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum*.

Bacchetta, M., Low, P., Mattoo, A., Schuknecht, L., Wager, H., and Wehrens, M. (1998). Electronic Commerce and the Role of the WTO (Special Studies 2). World Trade Organization.

Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). The

costs of data localisation: friendly fire on economic recovery. ECIPE Occasional Paper, 3, 2014.

Bieron, B., and Ahmed, U. (2012). Regulating E-Commerce through International Policy: Understanding the International Trade Law Issues of E-Commerce. *Journal of World T*rade, 46(3), 545-570.

Chander, A., & Le, U. P. (2014). Breaking the Web: Data Localization vs. the Global Internet. *Emory Law Journal, Forthcoming*.

Cooper, W. H., and Manyin, M. E. (2007). The proposed South Korea-US free trade agreement (KORUS FTA). Congressional Research Service, Library of Congress.

Delimatsis, Panagiotis. (2011). "Protecting Public Morals in a Digital Age: Revisiting the WTO Rulings on US–Gambling and China–Publications and Audiovisual Products." *Journal of International Economic Law*: jgr012.

Dix, A., Thüsing, G., Traut, J., Christensen, L., Etro, F., Aaronson, S. A., & Maxim, R. (2013). EU data protection reform: Opportunities and concerns.*Intereconomics*, *48*(5), 268-285.

Etro, F. (2010). The economics of cloud computing.

Hill, J. F. (2014). The growth of data localization post-snowden: Analysis and recommendations for us policymakers and business leaders. In The Hague Institute for Global Justice, Conference on the Future of Cyber Governance.

Horn, H., Mavroidis, P. C., and Sapir, A. (2010). "Beyond the WTO? An anatomy of EU and US preferential trade agreements." *The World Economy 33(11)*, 1565-1588.

King, Nancy J., and Kishani Kalupahana. "Choosing Between Liberalization and Regulatory Autonomy Under GATS: Implications of US-Gambling For Trade in Cross Border E-Services." *Vand. J. Transnat'l L.* 40 (2007): 1189.

Mishra, N. (2016) Data localization laws in a digital world. *The Public Sphere Journal*

Weber, Rolf H., Digital Trade in WTO-Law - Taking Stock and Looking Ahead (2010). *Asian Journal of WTO & International Health Law and Policy, Vol. 5, No. 1,* 1-24, March 2010. Available at SSRN:http://ssrn.com/abstract=1578139 or http://dx.doi.org/10.2139/ssrn.1578139

Van der Marel, E., Bauer, M., Lee-Makiyama, H., & Verschelde, B. (2016). A

methodology to estimate the costs of data regulations. International Economics, 146, 12-39.

Weber, Rolf H. (2015). Digital Trade and E-Commerce: Challenges and Opportunities of the Asia-Pacific Regionalism. *Asian Journal of WTO & International Health Law and Policy, Vol. 10, No. 2,* pp. 321-348, September 2015. Available at SSRN: http://ssrn.com/abstract=2669347

Korean Literature

박덕영. (2006). FTA와 전자상거래 분야 주요 쟁점. 서울국제법연구 제13권 2호, 95-102.

백수원. (2016). 프라이버시 보호를 위한 무인항공기 (드론) 규제 개선 방안 연구. 성균관 법학 제 28권 제 1호. 313-340

서민교. (2008). 전자상거래에 관한 한미 FTA의 평가와 향후 과제-KORUS FTA 제 15장을 중심으로. e-비즈니스연구 제 9권 2호, 87-110.

엄윤령. (2014). 위치정보보호법의 입법론적 개선방안 검토 – 위치정보의 정의 및 익명위치정보를 중심으로. 연세 의료 과학기술과 법 제 5권 제 2호, 52-80

이근화. (2016). 개정 정보기술협정 (ITA II) 발효 및 시사점. KITA 트레이드 포커스 연구보고서.

이한영. (2007). 디지털@통상협상-UR 에서 한미 FTA 까지. 서울: 삼성경제연구소.

이한영. (2008). 전자적 서비스무역에 관한 통상규범: WTO 및 FTA의 성과. 통상법률, 제 81 호, 119-146.

채대석, 김미정. (2011). E-Commerce의 확산과 WTO의 규정과 발전방안. 무역연구 제7권 3호, 193-214.

한민정. (2013). 한국의 TPP 참여전략에 관한 연구: 전자상거래를 중심으로. 통상정보연구 제15권 1호, 309-330.

Legal Texts

Act on the Establishment, Management, etc. of Spatial Data Article 16.

Act on the Protection, Use, Etc. of Location Information. Article 15.

KORUS FTA Article 15_

Personal Information Protection Act Article 17.

US-Peru FTA, Article 15.5

US-Colombia TA, Article 15.

Trans-Pacific Partnership Article 10

Trans-Pacific Partnership Article 14

Other texts

Kim J. H., Chung, B., Keh, S. K., and Lee, I. H. "Data protection in South

Korea: overview" https://content.next.westlaw.com/2-579

7926?transitionType=Default&contextData=(sc.Default)&__lrTS=2017050607

4209285&firstPage=true&bhcp=1, (July 15 2015)

“chance is low that Google would like to reapply for mapping data exportation to Korean government”
http://www.huffingtonpost.kr/2016/06/04/story_n_10293658.html (June 4 2016)

초록

급변하는 국제무역 관계 속에서 디지털 커머스는 무척 중요한 위치를 차지하게 되었다. 특히 데이터의 자유로운 이동은 국가를 막론하고 디지털 시대 국가발전의 중요한 요소라는 점에 이견이 없다. 하지만 아직도 많은 국가들은 국가간 데이터 이동을 법과 규제를 통해 제한하고 있고 이는 4차 산업혁명 시대에 중요한 산업인 LBS 산업, 클라우드 컴퓨팅 산업 등의 발전을 저해하고 있다. 한국 역시 개인정보보호법, 위치정보 보호법, 지도의 방출을 제한하는 법률 등을 통해 데이터 이동을 규제하고 있으며 이러한 데이터로컬리제이션 규제는 서비스 산업의 발전을 지연시키고 있다. 이러한 상황 속에서 데이터 이동과 데이터 서비스에 대한 WTO 수준의 다자간 논의는 발전하지 못하고 있고, 한미 FTA, 환태평양경제동반자협정 등의 FTA 채널에서의 논의가 이러한 이슈를 매우 중요하게, 그리고 상세하게 다루고 있다는 점에서 그 의의가 크다. 따라서 본 논문에서는 데이터로컬리제이션의 정의와 목적, 그리고 한국의 데이터규제와 관련된 법률에 대한 논의, 그리고 데이터로컬리제이션을 다루고 있는 FTA에 대한 심층적 분석을 통해 이 문제를 살펴보고자 한다.